English

Data protection, the need for information security

It is often required to transfer sensitive information of personal, financial or business nature. In these instances we want to ensure that this information is delivered securely and to the correct person. Physical delivery is more often impossible so electronic means are used. In this case, the transmissions are susceptible to eavesdropping (someone looking at the data) or interception (someone 'getting' the data) and/or alteration (someone changing the data). To counter these possible attacks encryption is used so that it is extremely difficult for intruders to see or get the data and even if they manage to see or capture it, they will not be able to understand it.

Encryption and decryption

Encryption is the process of converting information or data to some code or cipher which prohibits unauthorised access. There exists various algorithms of this conversion. The common elements of a conversion process are: 1) the data (also referred to as the plain text), 2)a secret value (referred to as the key or password), 3)an encryption algorithm (for the conversion from plain text to cipher) 4)the incomprehensible text (or cipher) and 5) the decryption algorithm (for the conversion of cipher back to original plain text. The schematic below gives a representation

Consider a simple example, a user called Bob needs to send some file to a user called Sue.

- Encryption: Bob will use the original plain text and a secret value as input to an encryption algorithm that will produce a cipher text (an incomprehensible sequence of characters). This cipher can then be emailed to Sue, and even if the transmission is intercepted the information cannot be extracted.
- Decryption: Sue receives the message and uses the cipher text and the same secret value as input to the decryption algorithm that will produce (as its output) the original plain text, which Sue can now use.

Types of encryption

Encryption can be symmetric when the key (secret value) used for encryption is the same as the one used for decryption. This usually means that sender and recipient will have to somehow share the key or have previously agreed on it.

Encryption can be asymmetric when one key is used for encryption and a different value is used for decryption. This type of encryption is also known as public-key encryption because of the approach followed for the encryption/decryption. Here is an example

1. Bob can use a piece of software to generate two keys. The algorithm is based on mathematics and the resulting keys can be used for either encrypting or decrypting so that when one key is used to encrypt the other can be used to decrypt.
2. Bob selects one of the two keys and marks this as his **private-key**. This key is kept private, not shared with anyone and safe guarded. The other key is marked as Bob's **public-key** and that key is made public and available to anyone (via a server or a trusted repository).
3. Now, Sue can download Bob's public key and can use it to encrypt a plain text message. The resulting cipher can be sent to Bob.
4. Bob can decrypt the message using the cipher text received from Sue and his private key. In this manner he will have the original plain text message from Sue.

In a similar fashion, user Sue can generate their pair of keys. Keep one private and make the other one public. When Bob wants to send some data to Sue, he can use Sue's public key and encrypt the data to produce the cipher. When the cipher is received by Sue, she can use her private key to decrypt the cipher and obtain the original plain text message from Bob. The capture below demonstrates the above scenario (Bob→ Sue)

Encryption for authentication

When using public-key encryption it can also act as an authentication to ensure that the sender of the message is actually who they say they are. Consider that Bob wants to send some information to Sue. The information is not sensitive but Sue must get it and be certain that the information is valid and coming from Bob.

Bob can use his private key to encrypt the plain text and then send the cipher to Sue. When Sue receives the cipher, the only way to see the message is to decrypt it using Bob's public key. This means that the message can only have been send from Bob as he is the only one having Bob's private key (which can only be decrypted using Bob's public key).